PN2-MB-RT 模块使用手册

-- V1.0

目录

一、产品概述

1.1、产品简介

PN2-MB-RT 是一款协议转换模块，是一款经济稳定、安装简易，适用性强的产品。

1.2、特点功能

- Profinet 和 Modbus 协议转换，Modbus 支持 ModbusRTU 和 ModbusTCP。
- 采用标准 Profinet 协议通信，可与 PLC、组态、上位机等进行组网
- 采用标准 Modbus 通信,可设置为 ModbusTCP 从站或者 ModbusTCP 主站，也可设置为 ModbusRTU 主站或者 ModbusRTU 从站。
- 作为 ModbusTCP 主站(ModbusTCP 客户端)时最多可连接 7 个 ModbusTCP 从站(ModbusTCP 服务器)。
- 作为 ModbusTCP 从站(ModbusTCP 服务器)时,最多可同时接受 5 个 ModbusTCP 主站(ModbusTCP 客户端)的连接和数据交互请求。
- ModbusRTU 通信端口可以选择使用 RS422 或者 RS485
- 支持常用的功能码，具体就是功能码 1,2,3,4,5,6,15,16。
- 最多支持 63 个命令节点，部分 PLC 可能只能支持一部分。
- 电源电路采用防反接设计
- 广泛用于工业现场 Modbus 设备的采集和控制

1.3、应用场景

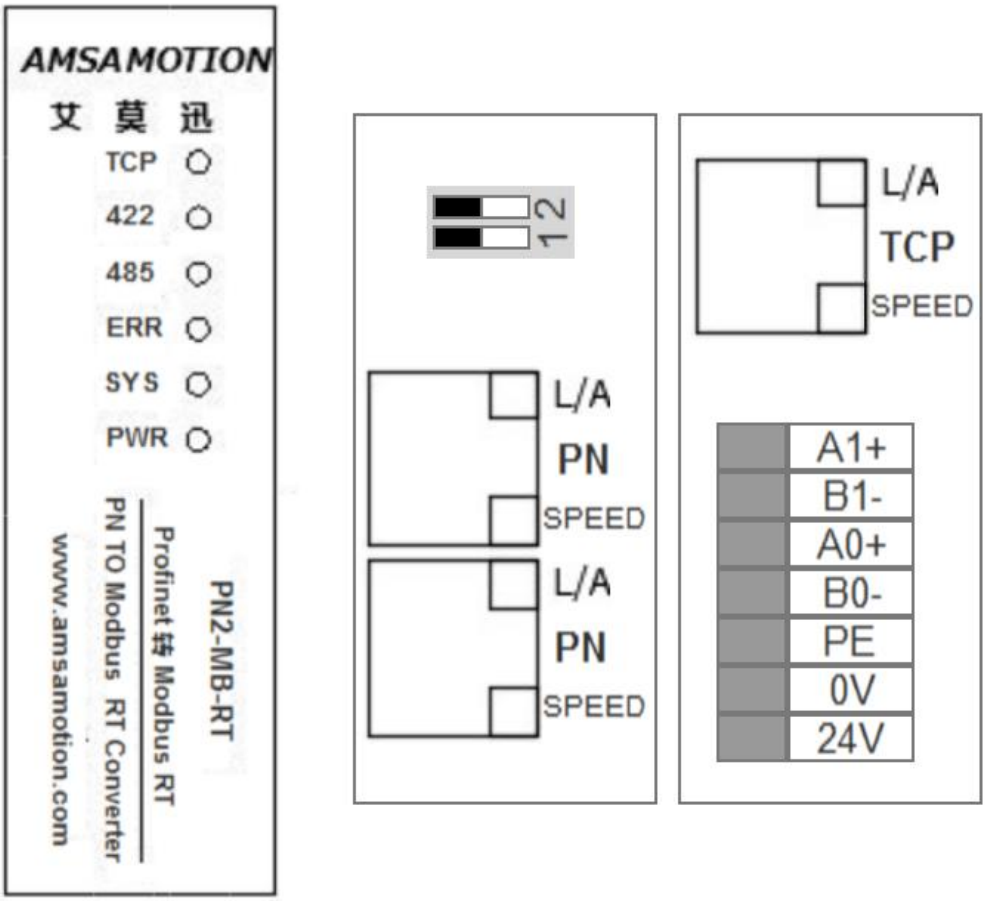
PN2-MB-RT 模块可应用范围很广，如：PLC 控制、工业自动化、楼宇自控、 POS 系统、电力监控、门禁医疗、考勤系统、自助银行系统、电信机房监控、信息家电、LED 信息显示设备、测量仪表及环境动力监控系统等设备或系统。

二、产品规格

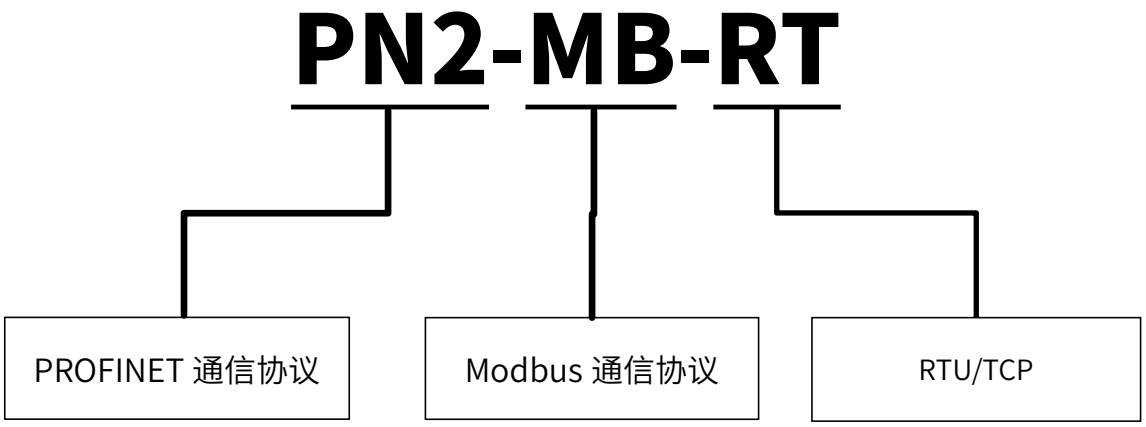
2.1、产品参数

网口参数	
接口类型	RJ45
通信协议	Profinet
最小通信周期	1ms
通信带宽	100Mbps
ModbusTCP 参数	
接口类型	RJ45
通信协议	ModbusTCP
最小通信周期	10ms
通信带宽	100Mbps
ModbusRTU 参数	
接口类型	RS422 或者 RS485
波特率	2400~4.6875Mbps
通信格式	默认 8 位数据，1 位停止，无校验
传输距离	波特率为 2400 时，串口通信 1200 米，以实际为准
其他	
安装方式	导轨
尺寸	125MM(长)*80MM(宽)*50MM(高)，以实物为准

2.2、外观说明



2.3、型号说明



2.4、端子说明

端子标号	功能说明
24V+	12-30V 直流供电电源正极
0V	12-30V 直流供电电源负极
PE	接地
B0-	RS422 接收反向端(RS485 反向端)
A0+	RS422 接收正向端(RS485 正向端)
B1-	RS422 发送反向端
A1+	RS422 发送正向端
两位拨码	1 号用于升级、2 号备用

2.5、指示灯说明

功能	LED 状态
上电后，LED 灯初始状态	SYS 灯 50ms 闪烁
校验错误，检查硬件加密芯片是否正常	所有灯光亮 200ms，灭 200ms，亮 200ms，灭 2000ms
周期性数据通信正常	SYS 灯 1000ms 闪烁
未进入周期性数据交换流程	SYS 灯 50ms 闪烁
模块查找	ERR 灯 200ms，灭 200ms，亮 200ms，灭 2000ms
升级模式功能	**升级 LED 状态**
升级模式初始化状态	SYS 灯常亮

	其他灯光 50ms 闪烁
文件传输完成，升级成功	SYS 常亮 其它灯光 50ms 闪烁
传输文件头出现错误（文件后缀错误、大小错误）	SYS 常亮 其它灯光亮 200ms 灭 200ms 亮 200ms 灭 200ms 亮 200ms 灭 2000ms
文件传输过程中	SYS 常亮 其它灯 1000ms 闪烁
文件传输失败（包丢失，或者校验错误）	SYS 常亮 其它灯亮 200ms，灭 200ms，亮 200ms，灭 2000ms
升级模式跳转运行模式失败	所有灯 200ms 灭 200ms 亮 200ms 灭 200ms 亮 200ms 灭 2000ms
硬件错误	所有灯常亮

三、产品功能

3.1、PN2-MB-RT 功能综述

本模块 使用 Modbus 主站功能时，每条命令以一定周期（可设）进行轮询，写功能调用不能小于轮询周期的 2 倍，不然会出现有一帧写功能数据未刷新的情况。(例如 Modbus 主站有 7 个命令结点，轮训间隔为 10ms，那么全部命令结点轮训完毕就得花费 70ms,则数据变化最小周期为 70ms*2=140ms)

使用 ModbusTCP 从站功能时，虽然可以同时响应 5 台主站的请求，但是考虑到单片机并发处理能力有限，所以每台主站轮训频率不能太快，太快会导致从站无法及时响应主站的请求，进而导致丢包以及主站报错。

3.2、修改 IP 地址

本模块 IP 地址可通过博图/step7 等软件进行修改，详细设置方式见第四章。

除此之外，还提供有专门软件进行快速修改 ip 等信息，详见文档《艾莫迅 PN 固件升级和 IP 修改工具使用说明书 .doc》。

3.3、升级功能

模块上电前，拨下升级按钮（拨码开关），直到 PN2-MB-RT 的 RUN 灯、ERR 灯、RS422、RS485 灯、TCP 灯均快速闪烁，模块即进入升级模式，升级模式详细说明见升级固件使用说明书。

四、使用博图 TIA 连接并使用本模块

本章节针对博图 TIA 连接 PN2-MB-RT 的过程进行介绍，以实现相应功能需求。

4.1、连接前准备

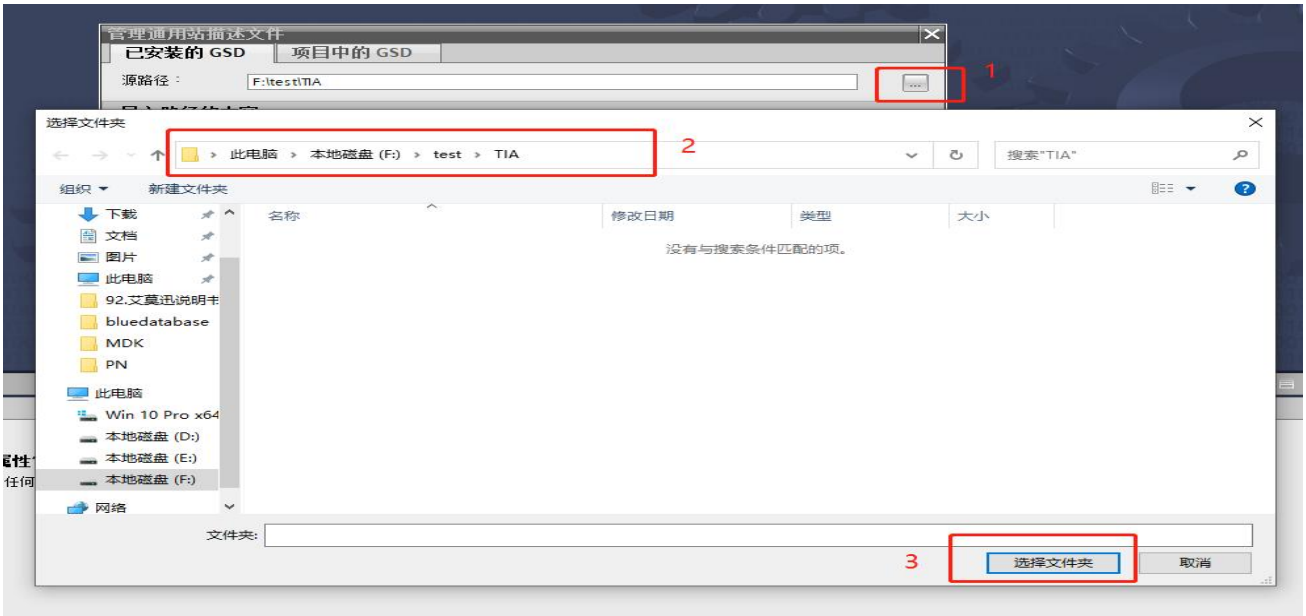
- 准备好 TIA 软件需要的 XML 文件，如下所示：

- 将 DC 24V 外部电源接入模块并通电，通电前请检查电源正负极是否连接正确。
- 使用网线将模块连接到 PLC 控制器的 Profinet 接口上。(在同一个网段)

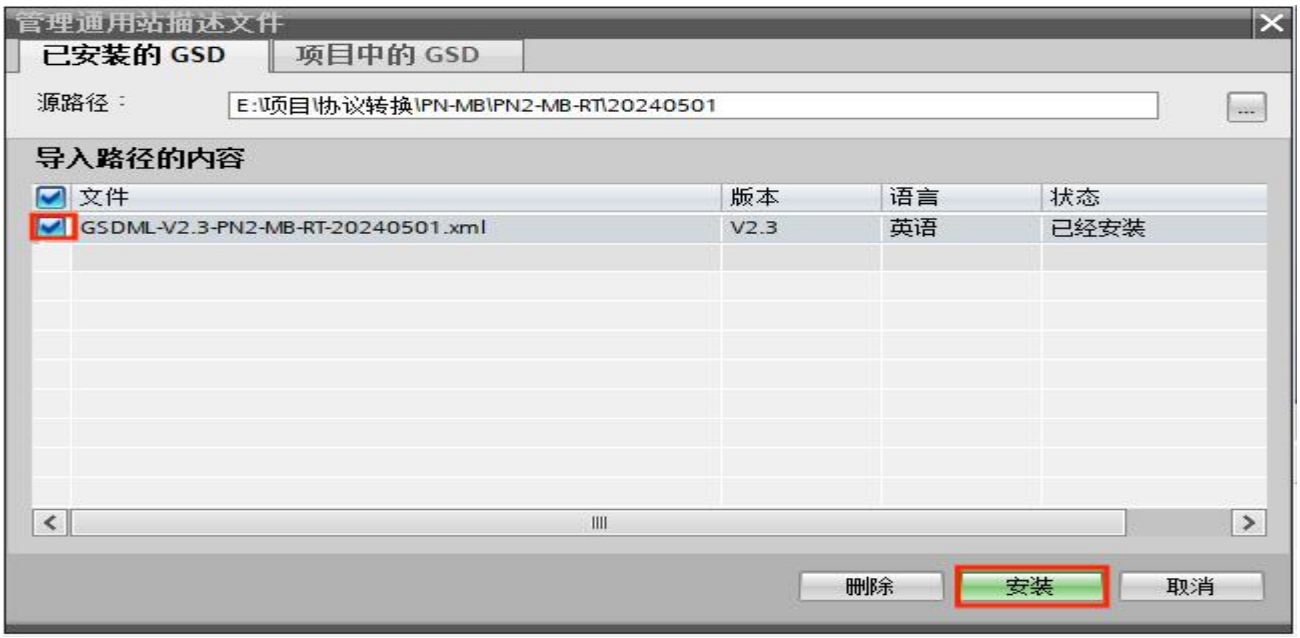
4.2、博图添加 GSDML 文件

●打开博图软件，选择项目视图，点击选项>管理通用站描述文件（GSD）(D)。

●在源路径中选择放置之前准备 GSDML 的文件夹，完成后点击选择文件夹，博图将自动扫描该文件夹下的 GSDML 文件。



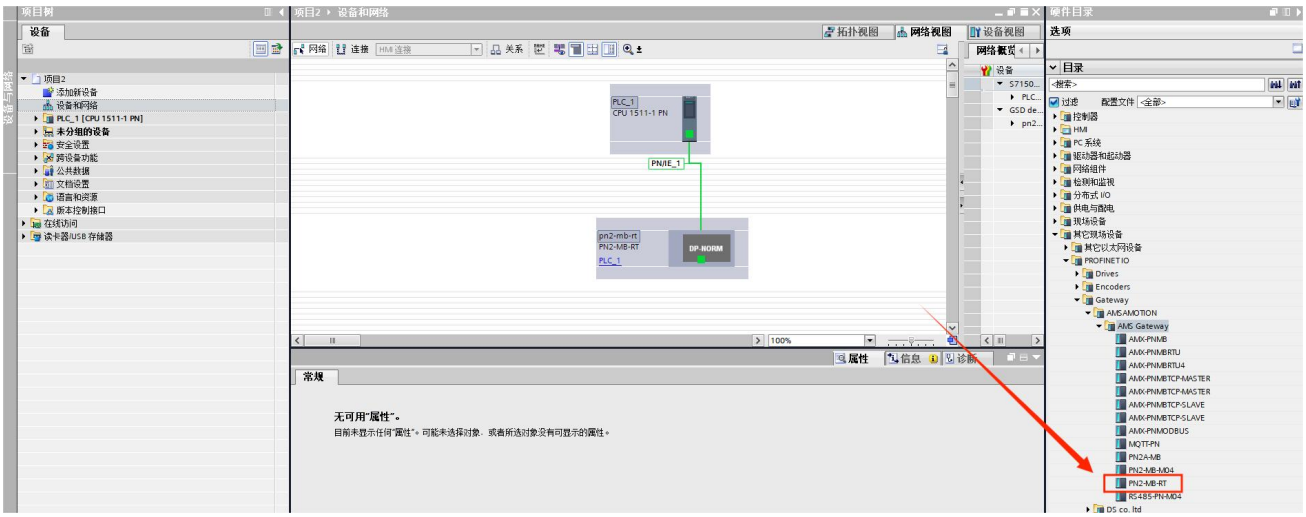
●点击要安装的 GSDML 文件左侧，勾选文件，后点击安装即可安装好相应的 GSDML 文件。



●安装完成后点击关闭，GSDML 文件安装成功。

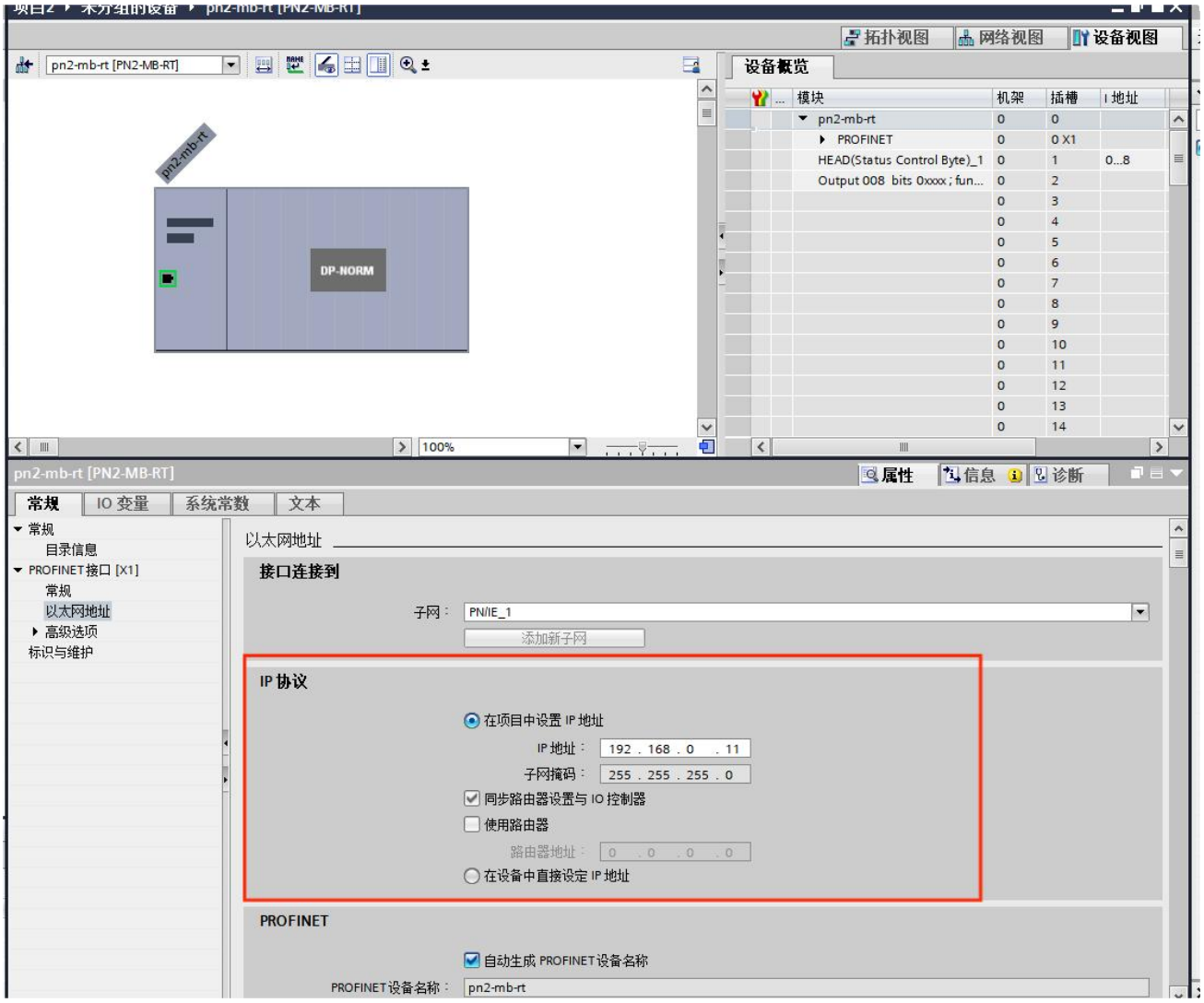
4.3、项目添加 PROFINET 设备

●新建或者打开项目，如果是新建项目，先添加控制器设备，然后在设备组态界面，添加相应 IO 模块，如下图：

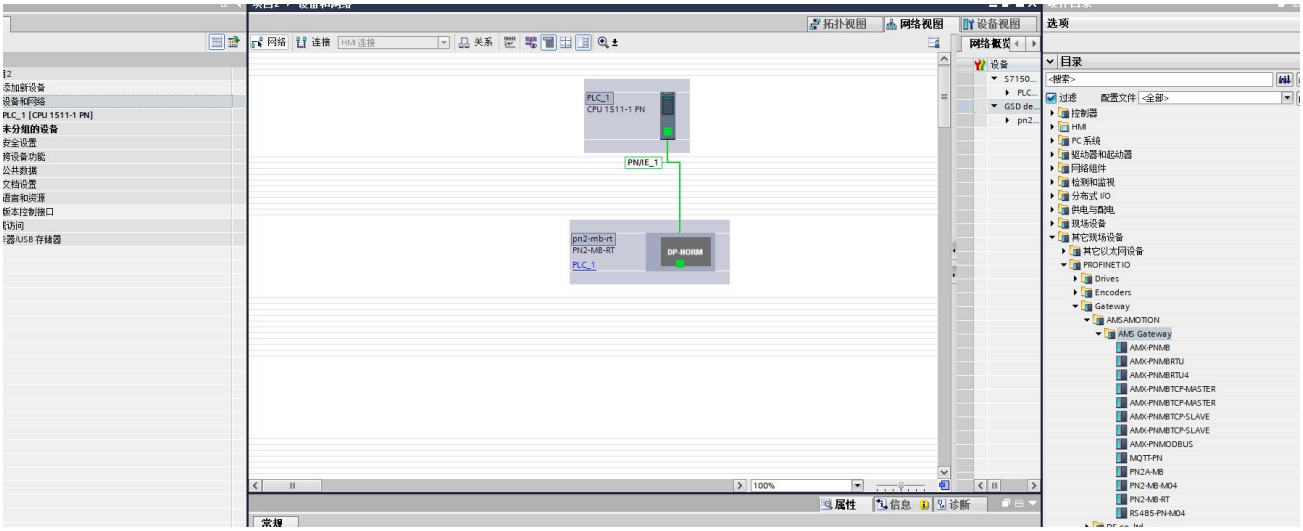


●在设备视图中选中刚添加的设备，双击图中模块，完成后修改常规中以太网地址选项卡，修改 IP 地址和设备名称，和模块本身保持一致。或者选用“在设备中直接设定 IP 地址”。

注意：未使用在设备中直接设定 IP 地址时，此时设置的 IP 地址和设备名称应和设备本身的保持一致，如果不清楚设备 IP 地址和设备名称，可以先随意设置，后将模块的 IP 地址和设备名称更改一致即可，修改模块的 IP 地址和设备名称请参照 4.5 节“博图修改模块名称和模块 IP 地址”。



●在网络视图中见添加的模块分配到 PLC 中：



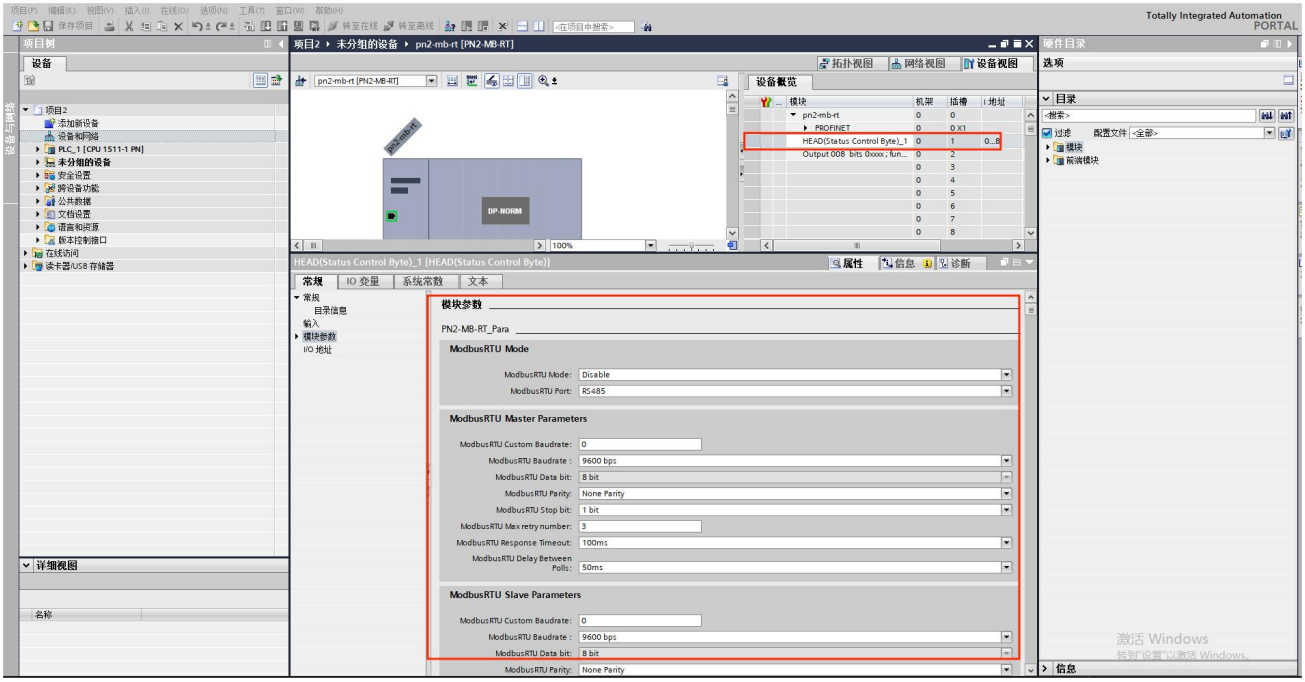
4.4、配置 Modbus 通信参数

我们的 PN2-MB-RT 网关既支持 ModbusTCP 主站和 ModbusTCP 从站，又支持 ModbusRTU 主站和 ModbusRTU 从站，具体通过 Profinet 的配置来决定。

●在拓扑视图界面选中 PN2-MB-RT 并双击,进入设备视图操作界面。

●在设备概览区域中，系统提供了 64 个槽位，其中第一号槽位为设备默认的设备状态字和设备控制字槽位 HEAD(Status Control Byte)_1，通过状态字 PLC 可以读取 Modbus 网关的运行状态，通过控制字 PLC 可以操作 Modbus 网关的运行。

●选中第一个槽位，选择属性，可以设定 PN-Modbus 的参数。



PN-Modbus 模块通信参数：

ModbusRTU Mode

--ModbusRTU Mode：

Disable： 表示关闭 ModbusRTU

As Master：表示设置 ModbusRTU 为主站

As Slave： 表示设置 ModbusRTU 为从站

--ModbusRTU Port：

RS485： 表示 ModbusRTU 使用 RS485 端口

RS422： 表示 ModbusRTU 使用 RS422 端口

ModbusRTU Master Parameters

--ModbusRTU Custom Baudrate：

设置 ModbusRTU 作为主站时的自定义波特率，默认为 0，为 0 表示自定义波特率不生效，此时下面的 ModbusRTU Baudrate 选项生效，自定义波特率取值范围为 1200~4687500。

--ModbusRTU Baudrate：

设置 ModbusRTU 作为主站时的标准波特率，当 ModbusRTU Custom Baudrate 为 0 时，这个标准波特率才生效。这里默认为 9600bps。

--ModbusRTU Data bit：

设定 ModbusRTU 作为主站时的数据位，可选择 8 位和 7 位。默认值为 8 位。

--ModbusRTU Parity：

设定 ModbusRTU 作为主站时的数据校验，可选择无校验(None Parity)，奇(Odd Parity)/偶(Even Parity)校验。默认为无校验。

--ModbusRTU Stop bit：

设定 ModbusRTU 作为主站时的数据停止位，可选择 1 位停止位，2 位停止位，0.5 位停止位或者 1.5 位停止位。默认值 1 位。

--ModbusRTU Max retry number：

设定 ModbusRTU 作为主站时的错误重试次数，0-255，0 不重发，255 无限重发，1-254 按次数重发。

--ModbusRTU Response Timeout：

ModbusRTU 作为主站时模块发出 Modbus 报文后，等待 Modbus 设备响应的时间，若 MODBUS 设备在设定的等待回答时间内仍无响应，模块停止等待，继续发送下一条 MODBUS 报文或重发。选择范围 10ms-1000ms 及无限期等待回答(Keep waiting...)。

--ModbusRTU Delay Between Polls：

ModbusRTU 作为主站时总线转换模块接收到 MODBUS 从站回复的正确报文后，延时发送 MODBUS 主站报文的时间。若 MODBUS 从站设备响应主站报文较慢，如果总线转换模块发送 MODBUS 报文过快，那么会出现通信故障，可以适当增加发送报文间隔时间。选择范围 10ms-1000ms 或者不等待（ No Delay）。默认值为 50 ms。

ModbusRTU Slave Parameters

--ModbusRTU Custom Baudrate：

设置 ModbusRTU 作为从站时的自定义波特率，默认为 0，为 0 表示自定义波特率不生效，此时下面的 ModbusRTU Baudrate 选项生效，自定义波特率取值范围为 1200~4687500。

--ModbusRTU Baudrate：

设置 ModbusRTU 作为从站时的标准波特率，当 ModbusRTU Custom Baudrate 为 0 时，这个标准波特率才生效。这里默认为 9600bps。

--ModbusRTU Data bit：

设定 ModbusRTU 作为从站时的数据位，可选择 8 位和 7 位。默认值为 8 位。

--ModbusRTU Parity：

设定 ModbusRTU 作为从站时的数据校验，可选择无校验(None Parity)，奇(Odd Parity)/偶(Even Parity)校验。默认为无校验。

--ModbusRTU Stop bit：

设定 ModbusRTU 作为从站时的数据停止位，可选择 1 位停止位，2 位停止位，0.5 位停止位或者 1.5 位停止位。默认值 1 位。

--ModbusRTU Delay Response Time：

设定 ModbusRTU 作为从站时接收到主站发过来的轮询命令后，延迟多长时间才进行回复。可填 0~65535,0 表示立即回复，单位是 ms。

ModbusRTU Slave Address(1..247)：

设定 ModbusRTU 作为从站时的站地址。可填 1~247，默认为 1。

ModbusTCP Mode

--ModbusTCP Mode：

Disable： 表示关闭 ModbusTCP

As Master：表示设置 ModbusTCP 为主站

As Slave： 表示设置 ModbusTCP 为从站

ModbusTCP Master Parameters

--IP Mode：

ModbusTCP 主站的 IP 模式: 1.可以选择 Dynamic IP 即动态 IP，此时 ModbusTCP 对应的网口得提前使用网线和路由器连接，使用 DHCP 自动从路由器获取 IP 地址，子网掩码，网关地址和 DNS 服务器地址。也就是说 IP Mode 下面的 Static IP，Subnet Mask，Router IP 和 DNS Server IP 不用填写。2.也可以选择 Static IP 即静态 IP，那么此时 Static IP，Subnet Mask，Router IP 和 DNS Server IP 这 4 个选项都得手动填写。

--Static IP1 ~ Static IP4：

静态 IP 模式下，ModbusTCP 主站自身的 IP 地址。

--Subnet Mask1 ~ Subnet Mask4：

静态 IP 模式下，ModbusTCP 主站自身的子网掩码，一般为 255.255.255.0。

--Router IP1 ~ Router IP4：

静态 IP 模式下，ModbusTCP 主站自身的路由器 IP 地址。

--DNS Server IP1 ~ DNS Server IP4：

静态 IP 模式下，ModbusTCP 主站自身的 DNS 服务器 IP 地址。

这里说明一下 ModbusTCP 自身的 IP 地址可以通过读取 Modbus 的运行状态中的第 2,3,4,5 字节获知(第一字节保留未用)。

--ModbusTCP Max retry number of times：

设定错误重试次数，0-255，0 不重发，255 无限重发，1-254 按次数重发。

--ModbusTCP Response Timeout：

ModbusTCP 主站发出 ModbusTCP 报文后，等待 ModbusTCP 设备响应的时间，若 ModbusTCP 设备在设定的等待回答时间内仍无响应，ModbusTCP 主站停止等待，进行重发或者继续发送下一条 ModbusTCP 报文。

选择范围 10ms-1000ms 及无限期等待回答（ Keep waiting…）。

--ModbusTCP Delay Between Polls：

ModbusTCP 主站接收到 ModbusTCP 从站回复的正确报文后，延时发送下一个 ModbusTCP 报文的时间。若 ModbusTCP 从站设备响应主站报文较慢，如果 ModbusTCP 主站发送 ModbusTCP 报文过快，那么会出现通信故障，可以适当增加发送报文间隔时间。

选择范围 10ms-1000ms 或者不等待（ No Delay）。 默认值为 10 ms。

因为 ModbusTCP 主站可以同时连接 7 个 ModbusTCP 从站，所以下面有 7 组从站参数分别对应 ModbusTCP 从站 1~ModbusTCP 从站 7，下面仅就 ModbusTCP 从站 1 进行说明。

--ModbusTCP Slave1 Unit Identifier(1-247)：

就是要访问的 ModbusTCP 从站设备的站地址，可填写值 1~247。

--ModbusTCP Slave1 IP1 ~ ModbusTCP Slave1 IP4：

就是 ModbusTCP 从站设备的 IP 地址，得和 ModbusTCP 主站处于同一网段。

ModbusTCP Slave Parameters

--IP Mode：

ModbusTCP 从站的 IP 模式: 1.可以选择 Dynamic IP 即动态 IP，此时 ModbusTCP 对应的网口得提前使用网线和路由器连接，使用 DHCP 自动从路由器获取 IP 地址，子网掩码，网关地址和 DNS 服务器地址。也就是说 IP Mode 下面的 Static IP，Subnet Mask，Router IP 和 DNS Server IP 不用填写。2.也可以选择 Static IP 即静态 IP，那么此时 Static IP，Subnet Mask，Router IP 和 DNS Server IP 这 4 个选项都得手动填写。

--Static IP1 ~ Static IP4：

静态 IP 模式下，ModbusTCP 从站自身的 IP 地址。

--Subnet Mask1 ~ Subnet Mask4：

静态 IP 模式下，ModbusTCP 从站自身的子网掩码，一般为 255.255.255.0。

--Router IP1 ~ Router IP4：

静态 IP 模式下，ModbusTCP 从站自身的路由器 IP 地址。

--DNS Server IP1 ~ DNS Server IP4：

静态 IP 模式下，ModbusTCP 从站自身的 DNS 服务器 IP 地址。

这里说明一下 ModbusTCP 自身的 IP 地址可以通过读取 Modbus 的运行状态中的第 2,3,4,5 字节获知(第一字节保留未用)。

--ModbusTCP Slave Unit Identifier(1-247)：

就是设定 ModbusTCP 从站设备的站地址，可填写值 1~247。

--ModbusTCP Slave Response delay Time：

设定 ModbusTCP 作为从站时接收到主站发过来的轮询命令后，延迟多长时间才进行回复。可填 0~65535，单位是 ms。

4.5、配置 Modbus 状态字和控制字

从设备概览配置中可以看到槽号 1 被系统自动占用(HEAD(Status Control Byte)_1)，其中 I 地址一栏中，对应的 PROFINET 输入地址 IB1-IB9（可改），为通信状态监控字。Q 地址一栏中，对应的 PROFINET 输出地址 QB1-QB9（可改），QB1 为 Modbus 网关设备的通信控制字，QB2-QB9 为每条报文发送的控制字。

Modbus 的通信状态监控字：

第 1 字节：保留未使用

第 2 字节：ModbusTCP 主站的 IP 地址第 1 字节(比如主站的 IP 地址为 192.168.0.100。那么此字节就表示 192)。

第 3 字节：ModbusTCP 主站的 IP 地址第 2 字节(比如主站的 IP 地址为 192.168.0.100。那么此字节就表示 168)。

第 4 字节：ModbusTCP 主站的 IP 地址第 3 字节(比如主站的 IP 地址为 192.168.0.100。那么此字节就表示 0)。

第 5 字节：ModbusTCP 主站的 IP 地址第 4 字节(比如主站的 IP 地址为 192.168.0.100。那么此字节就表示 100)。

其他字节保留。

Modbus 的控制字：

第一字节 QB1：

Bit 0：ModbusTCP 主站 1 和 ModbusTCP 从站使能位，1 = 启用，0 = 不启用。

Bit 1：ModbusTCP 主站 2 使能位，1 = 启用，0 = 不启用。

Bit 2：ModbusTCP 主站 3 使能位，1 = 启用，0 = 不启用。

Bit 3：ModbusTCP 主站 4 使能位，1 = 启用，0 = 不启用。

Bit 4：ModbusTCP 主站 5 使能位，1 = 启用，0 = 不启用。

Bit 5：ModbusTCP 主站 6 使能位，1 = 启用，0 = 不启用。

Bit 6：ModbusTCP 主站 7 使能位，1 = 启用，0 = 不启用。

Bit 7：ModbusRTU 主站和 ModbusRTU 从站使能位，1 = 启用，0 = 不启用。

正常使用时直接往第 1 字节中写入 255，即 8 个 1。

第 2 字节到第 9 字节：

每一个槽的报文对应一位。对应形式如下表。

当报文配置为上升沿触发时（见 4.6 章节 报文设置），将该位由 0->1 时，报文启用一次发送。

当报文配置为电平触发模式（见 4.6 章节 报文设置）。将该位置 1 时，对于写类型的功能码仅当数据发生变化时才发送，对于读类型的功能码会直接发送；置 0 时，报文停止发送。

--第 2 字节：

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
插槽 8	插槽 7	插槽 6	插槽 5	插槽 4	插槽 3	插槽 2	空

--第 3 字节：

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
插槽 16	插槽 15	插槽 14	插槽 13	插槽 12	插槽 11	插槽 10	插槽 9

--第 4 字节：

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
插槽 24	插槽 23	插槽 22	插槽 21	插槽 20	插槽 19	插槽 18	插槽 17

--第 5 字节：

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
插槽 32	插槽 31	插槽 30	插槽 29	插槽 28	插槽 27	插槽 26	插槽 25

--第 6 字节：

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
插槽 40	插槽 39	插槽 38	插槽 37	插槽 36	插槽 35	插槽 34	插槽 33

--第 7 字节：

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
插槽 48	插槽 47	插槽 46	插槽 45	插槽 44	插槽 43	插槽 42	插槽 41

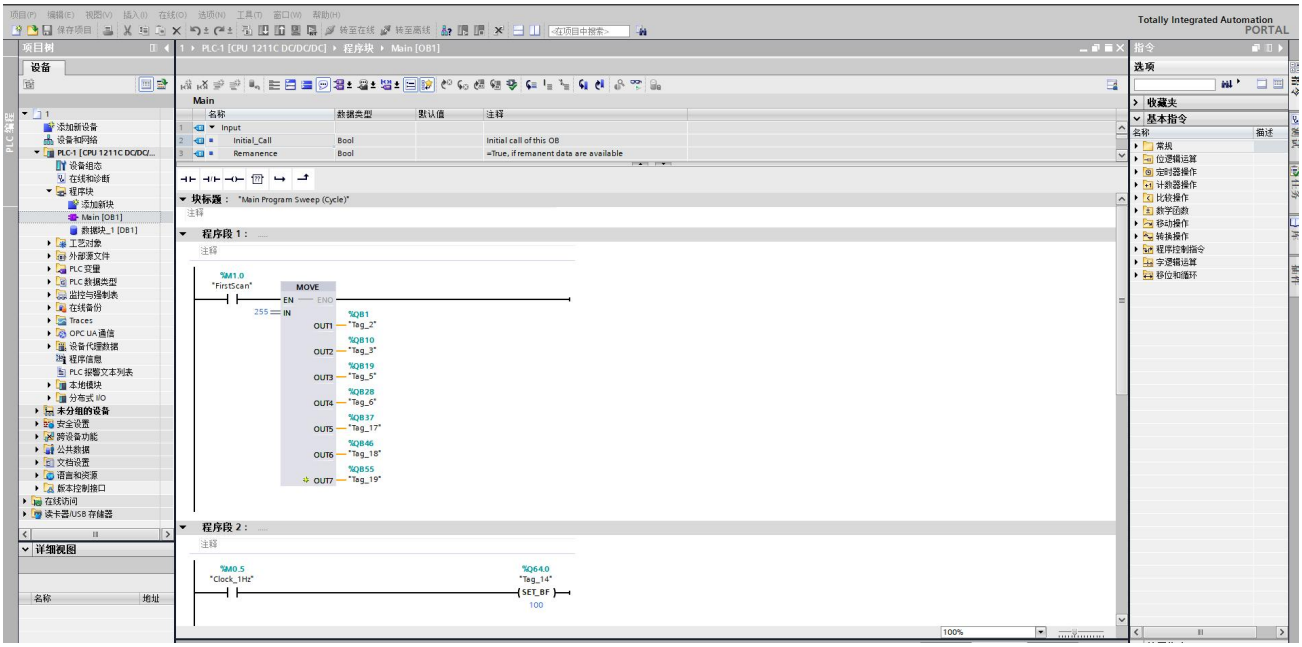
--第 8 字节：

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
插槽 56	插槽 55	插槽 54	插槽 53	插槽 52	插槽 51	插槽 50	插槽 49

--第 9 字节：

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
插槽 64	插槽 63	插槽 62	插槽 61	插槽 60	插槽 59	插槽 58	插槽 57

给 modbus 设备使能信号（不给使能信号无法使用）



4.6 配置 Modbus 报文（功能码）

在设备概览中一共有 64 个槽位,第一个个槽作为状态字和控制字已被占用，剩下 63 个槽位可供配置 MODBUS 报文（命令）。每个槽可以用来插入一条 MODBUS 通信报文（命令）,所以一共可以插入 63 个 MODBUS 通信报文（命令）。

单击右侧硬件目录中的模块有八个 Modbus 地址操作文件夹。前四个表示 Modbus 主站专用，后四个表示 Modbus 从站专用。单击每个文件夹，可以选择里面的相应 Modbus 命令。

直接左键双击硬件目录中的 Modbus 命令，就可以按照空白的槽位顺序将报文配置到 MODBUS 报文队列中。

每条 Modbus 主站命令有 5 个属性。

—Modbus Master Port：可选 ModbusRTU 或者 ModbusTCP Slave1~ModbusTCP Slave7 表示当前的 Modbus 命令结点会从那个端口发出。

—ModbusRTU Slave Address(1..247)：当上面选择 ModbusRTU 时才生效，表示 ModbusRTU 从站的地址。

—Function Code：Modbus 主站的功能码，根据插入插槽的 MODBUS 命令自动生成功能码，不可更改。

—Start Address(0-65535)：对 Modbus 从站数据操作的开始地址，范围是 0~65535。

—Quantity of Write（或者 Quantity of Read，Quantity Of Register）：表示读写的寄存器或者线圈的数量。

—Transmission Type：提供 4 种发送类型。

disable(命令失能)：表示命令不发送，即命令失能。

Poll trigger（轮询发送）： 控制字中的相应位置位后，该报文会按照插槽号从小到大的顺序依次发送。此发送方式下，读/写指令均会强制执行，不管写指令时数据是否改变。默认此模式。

Level trigger（电平发送）： 槽号对应的控制发送标志位由 0 变到 1 后：对于读指令，该报文会被发送。对于写指令，如果数据有改变才会执行；槽号对应的控制发送标志位由 1 变到 0 后，不论是读报文还是写报文都会停止发送。

Rising trigger（上升沿发送）： 槽号对应的触发控制位由 0 变到 1 后，该报文会发送一次。此发送方式下，读写指令均只有检测到对应槽的触发控制位的上升沿后，才会执行一次。

Modbus 主站支持下面八个 MODBUS 通信命令

功能码	功能	操作地址区域（非寄存器 PLC 地址）	操作类型
01H	读取多个线圈输出状态	0XXXX	读
02H	读取多个输入线圈状态	1XXXX	读
03H	读取多个保存寄存器	4XXXX	读
04H	读取输入寄存器	3XXXX	读
05H	强置单个线圈	0XXXX	写
06H	预置单个保持寄存器	4XXXX	写
0FH	强置多线圈	0XXXX	写
10H	预置多个保持寄存器	4XXXX	写

Modbus 从站每个报文命令只有一个参数需要配置。

—Modbus Slave Port：

ModbusRTU 表示数据通过 RS485 或者 RS422 进行交互

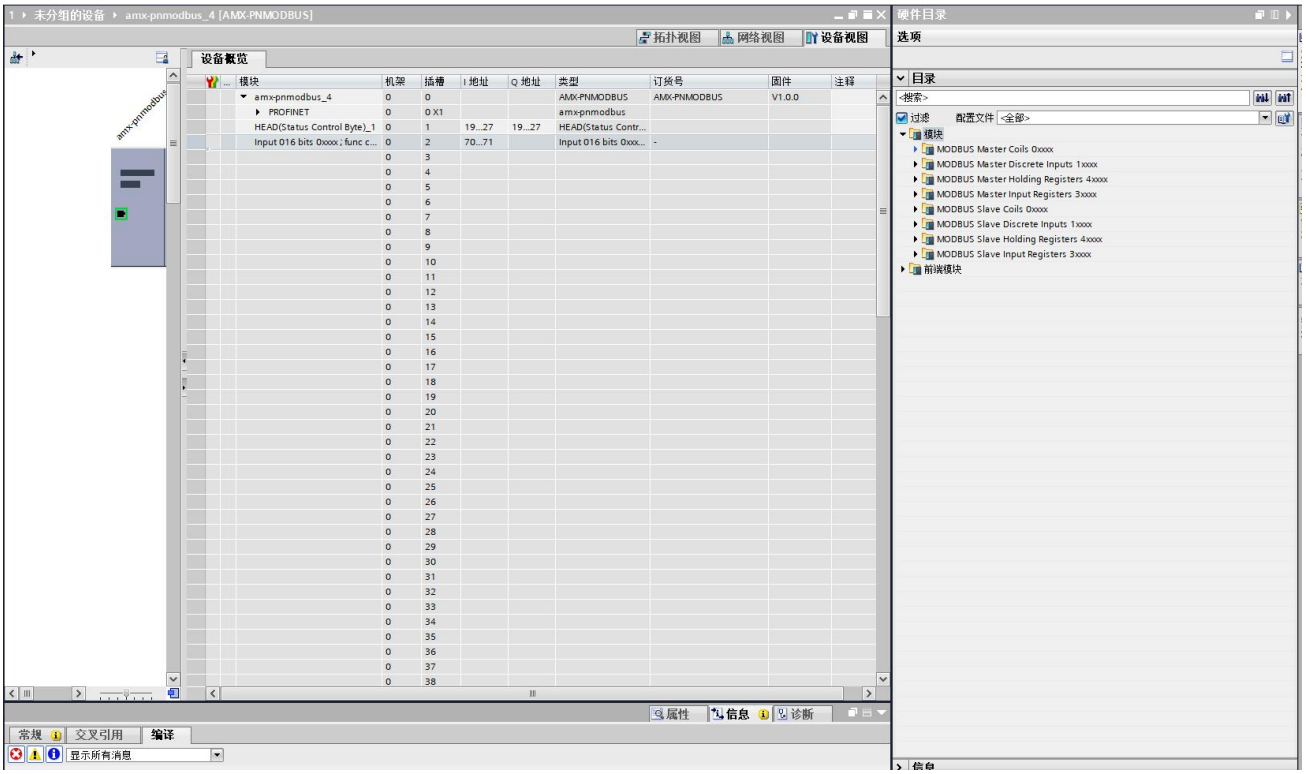
ModbusTCP 表示数据通过网口进行交互

硬件目录的模块里面的 4 个从站文件夹得说明一下

4 个从站文件夹里面装的是对应的 Modbus 从站报文功能码，每个报文功能码前缀是 Output 或者 Input。Output 是相对 PLC 来讲的，即 PLC 通过 Profinet 发送数据给 PN-Modbus 网关，Modbus 主站来读取这些数据，Input 也是相对于 PLC 来讲的，Modbus 主站发送数据给 ModbusTCP 从站，ModbusTCP 从站通过 Profinet 将数据发送给 PLC。也即 Output 表示读类型的功能码，Input 表示写类型的功能码。并且每个报文功能码后面附有它表示的具体功能码号码，比如 Output 01 Words 3xxx;fun code 4 表示读一个输入寄存器。

这里得注意一点就是这 63 个槽里面最好不要有功能码相同的报文，如果功能码相同就算是重复了，那么重复的功能码中就会存在有的功能码不会被执行。

根据需求选择主站还是从站然后添加需要的功能码



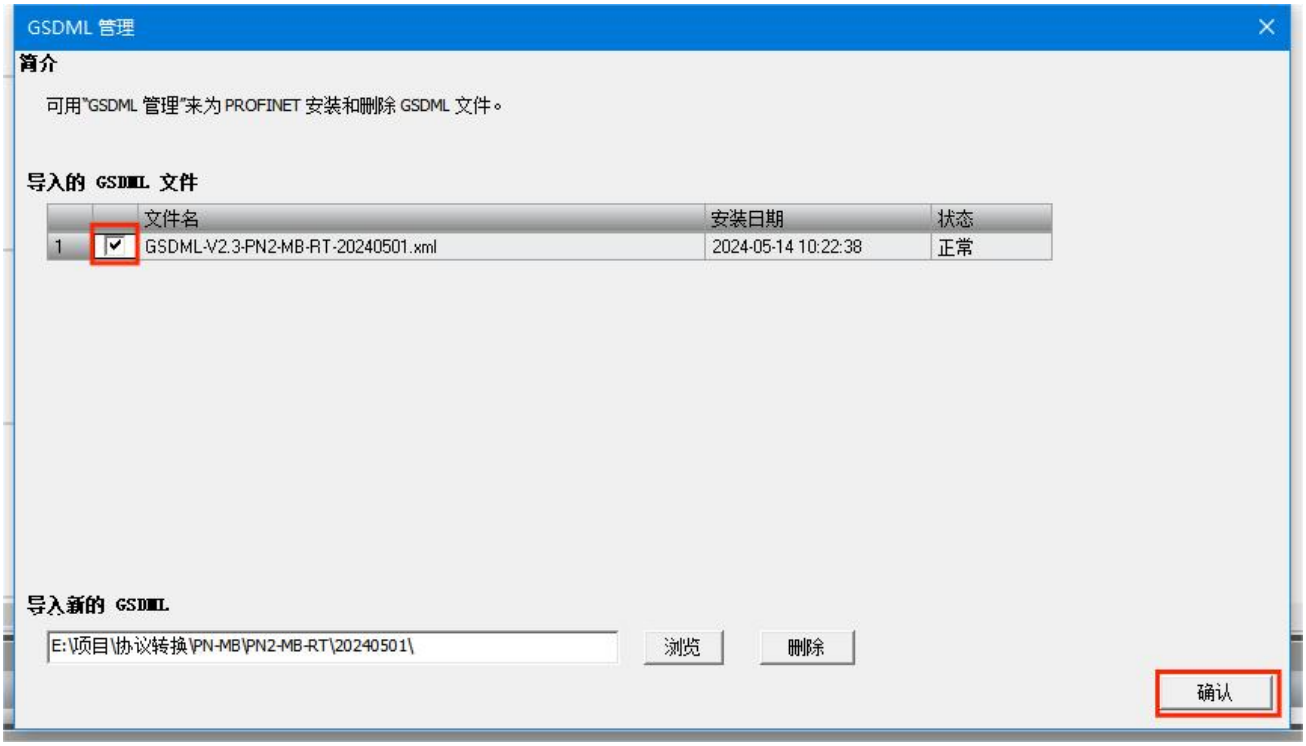
五、STEP 7-MicroWIN SMART 连接并使用模块

5.1、连接前准备

- 准备好 TIA 软件需要的 XML 文件，如下所示：

- 将 DC 24V 外部电源接入模块并通电，通电前请检查电源正负极是否连接正确。
- 使用网线将模块连接到 PLC 控制器的 Profinet 接口上。(在同一个网段)

5.2、STEP 7-MicroWIN SMART 添加 GSDML 文件

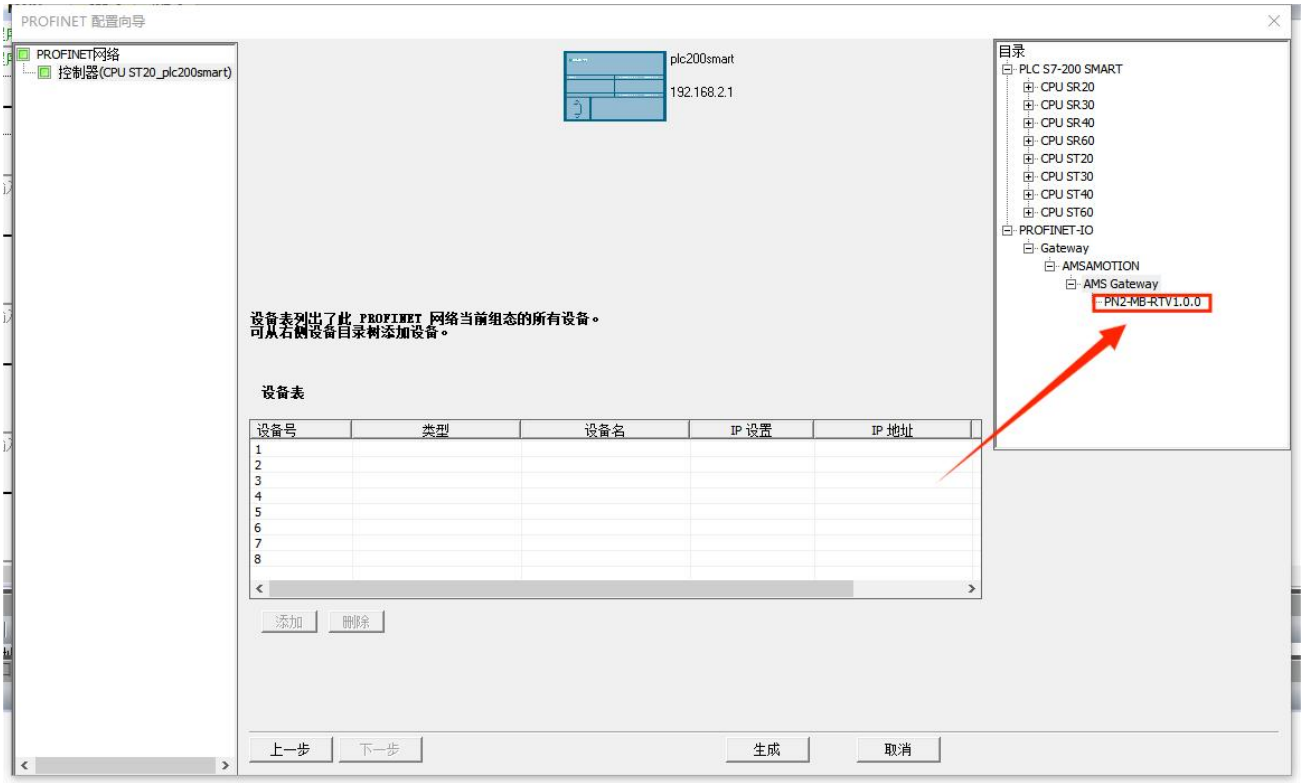


5.3、项目添加 PROFINET 设备

●选择工具菜单下面的 PROFINET 命令

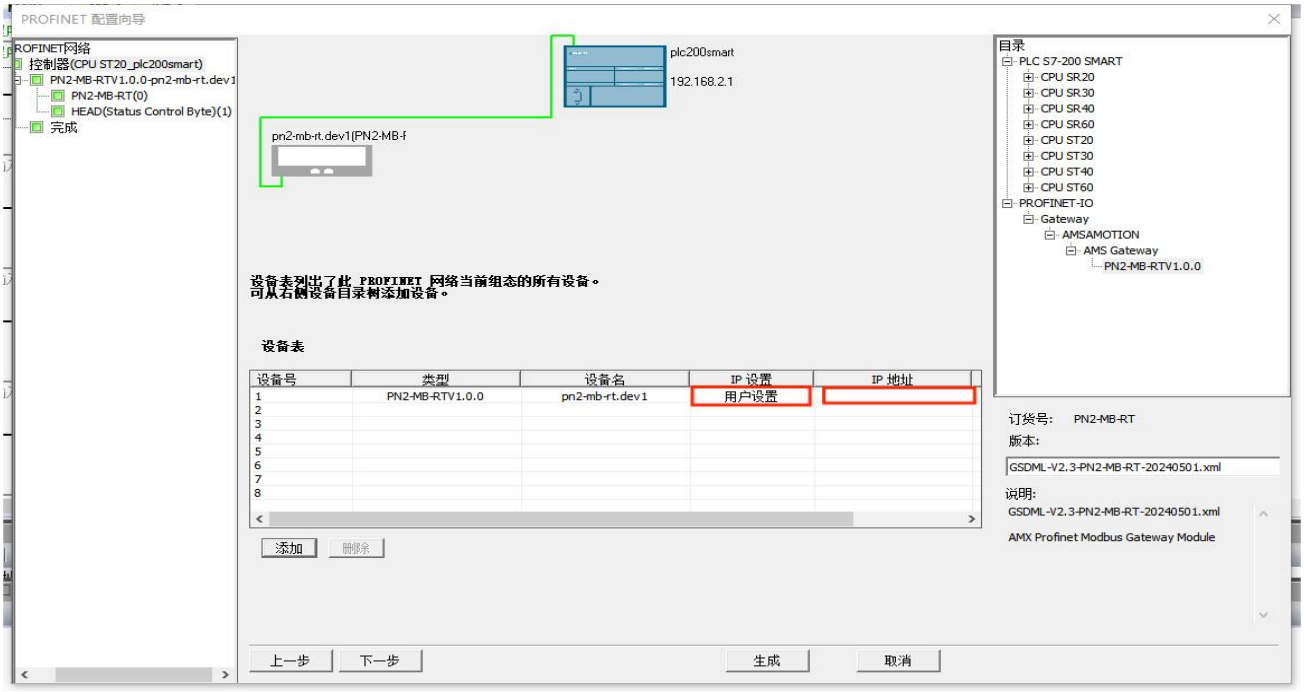
●选择 PLC 角色为 PLC 控制器，设置对应 PLC 控制器 IP 等相关参数。完成后点击下一步。

●在右边栏中 PROFINET-IO>I/O>AMSAMOTION>Profinet I/O 下选择 PN2-MB-RT 单击选中，然后按住左键，将其拖拽到左侧表格内。



●双击设备名栏，填入相应设备名称，同一项目内不能有相同的设备名，同样设置 IP 地址，保持和 PLC 控制器在同一网段内。

注意：此时设置的设备名需要和设备保持一致，如果不清楚设备名，可以先随意设置，后将模块的设备名更改一致即可，此时设置的 IP 地址会在组态时，将同设备名的模块的 IP 设置成这里设置的值。设备名称修改请参照 5.5 节“STEP 7-MicroWIN SMART 修改模块名称和模块 IP 地址”。



5.4、配置 Modbus 报文（功能码）

在设备概览中一共有 64 个槽位,第一个个槽作为状态字和控制字已被占用，剩下 63 个槽位可供配置 MODBUS 报文（命令）。每个槽可以用来插入一条 MODBUS 通信报文（命令）,所以一共可以插入 63 个 MODBUS 通信报文（命令）。

单击右侧硬件目录中的模块有八个 Modbus 地址操作文件夹。前四个表示 Modbus 主站专用，后四个表示 Modbus 从站专用。单击每个文件夹，可以选择里面的相应 Modbus 命令。

直接左键双击硬件目录中的 Modbus 命令，就可以按照空白的槽位顺序将报文配置到 MODBUS 报文队列中。

每条 Modbus 主站命令有 5 个属性。

—Modbus Master Port：可选 ModbusRTU 或者 ModbusTCP Slave1~ModbusTCP Slave7 表示当前的 Modbus 命令结点会从那个端口发出。

—ModbusRTU Slave Address(1..247)：当上面选择 ModbusRTU 时才生效，表示 ModbusRTU 从站的地址。

—Function Code：Modbus 主站的功能码，根据插入插槽的 MODBUS 命令自动生成功能码，不可更改。

—Start Address(0-65535)：对 Modbus 从站数据操作的开始地址，范围是 0~65535。

—Quantity of Write（或者 Quantity of Read，Quantity Of Register）：表示读写的寄存器或者线圈的数量。

—Transmission Type：提供 4 种发送类型。

disable(命令失能)：表示命令不发送，即命令失能。

Poll trigger（轮询发送）： 控制字中的相应位置位后，该报文会按照插槽号从小到大的顺序依次发送。此发送方式下，读/写指令均会强制执行，不管写指令时数据是否改变。默认此模式。

Level trigger（电平发送）： 槽号对应的控制发送标志位由 0 变到 1 后：对于读指令，该报文会被发送。对于写指令，如果数据有改变才会执行；槽号对应的控制发送标志位由 1 变到 0 后，不论是读报文还是写报文都会停止发送。

Rising trigger（上升沿发送）： 槽号对应的触发控制位由 0 变到 1 后，该报文会发送一次。此发送方式下，读写指令均只有检测到对应槽的触发控制位的上升沿后，才会执行一次。

Modbus 主站支持下面八个 MODBUS 通信命令

功能码	功能	操作地址区域（非寄存器 PLC 地址）	操作类型
01H	读取多个线圈输出状态	0XXXX	读
02H	读取多个输入线圈状态	1XXXX	读
03H	读取多个保存寄存器	4XXXX	读
04H	读取输入寄存器	3XXXX	读
05H	强置单个线圈	0XXXX	写
06H	预置单个保持寄存器	4XXXX	写
0FH	强置多线圈	0XXXX	写
10H	预置多个保持寄存器	4XXXX	写

Modbus 从站每个报文命令只有一个参数需要配置。

—Modbus Slave Port：

ModbusRTU 表示数据通过 RS485 或者 RS422 进行交互

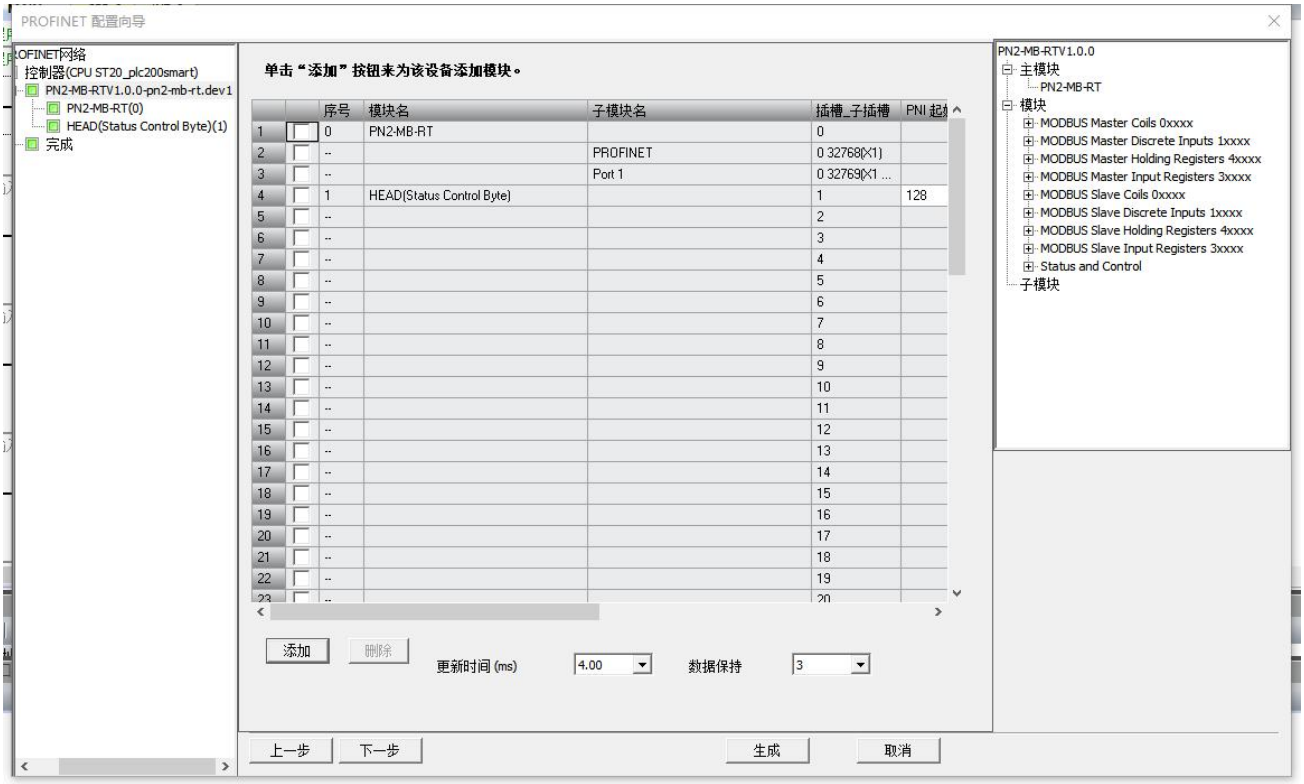
ModbusTCP 表示数据通过网口进行交互

硬件目录的模块里面的 4 个从站文件夹得说明一下

4 个从站文件夹里面装的是对应的 Modbus 从站报文功能码，每个报文功能码前缀是 Output 或者 Input。Output 是相对 PLC 来讲的，即 PLC 通过 Profinet 发送数据给 PN-Modbus 网关，Modbus 主站来读取这些数据，Input 也是相对于 PLC 来讲的，Modbus 主站发送数据给 ModbusTCP 从站，ModbusTCP 从站通过 Profinet 将数据发送给 PLC。也即 Output 表示读类型的功能码，Input 表示写类型的功能码。并且每个报文功能码后面附有它表示的具体功能码号码，比如 Output 01 Words 3xxx;fun code 4 表示读一个输入寄存器。

这里得注意一点就是这 63 个槽里面最好不要有功能码相同的报文，如果功能码相同就算是重复了，那么重复的功能码中就会存在有的功能码不会被执行。

根据需求选择主站还是从站然后添加需要的功能码



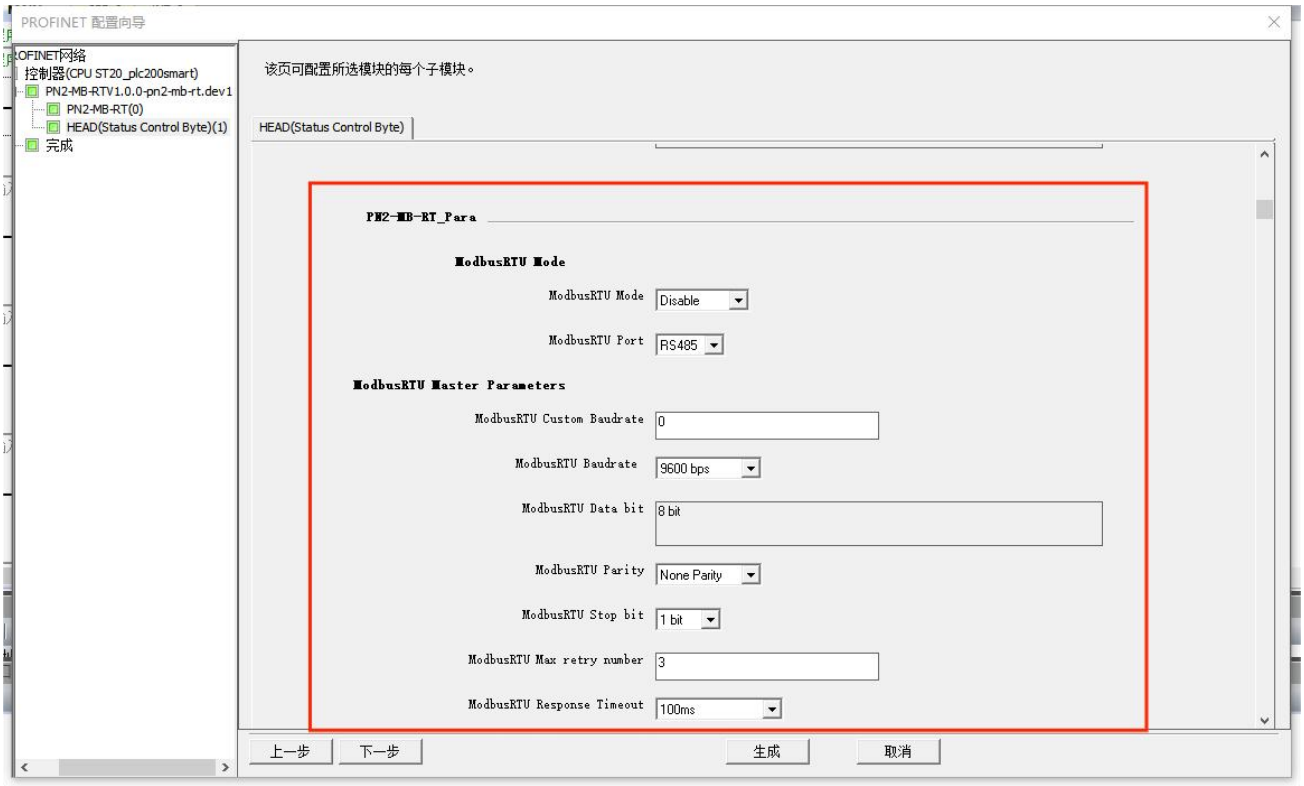
5.5、配置 Modbus 通信参数

我们的 PN2-MB-RT 网关既支持 ModbusTCP 主站和 ModbusTCP 从站，又支持 ModbusRTU 主站和 ModbusRTU 从站，具体通过 Profinet 的配置来决定。

●*在拓扑视图界面选中 AMX-MBTCP 并双击,进入设备视图操作界面。*

●*在设备概览区域中，系统提供了 64 个槽位，其中第一号槽位为设备默认的设备状态字和设备控制字槽位 HEAD(Status Control Byte)_1，通过状态字 PLC 可以读取 Modbus 网关的运行状态，通过控制字 PLC 可以操作 Modbus 网关的运行。*

●选中第一个槽位，选择属性，可以设定 PN-Modbus 的参数。（详情请看 4.4）



5.6、配置 Modbus 状态字和控制字

从设备概览配置中可以看到槽号 1 被系统自动占用(HEAD(Status Control Byte)_1)，其中 I 地址一栏中，对应的 PROFINET 输入地址 IB128-IB136（可改），为通信状态监控字。Q 地址一栏中，对应的 PROFINET 输出地址 QB128-QB136（可改），QB128 为 Modbus 网关设备的通信控制字，QB129-QB136 为每条报文发送的控制字。

Modbus 的通信状态监控字：

第 1 字节：保留未使用

第 2 字节：ModbusTCP 主站的 IP 地址第 1 字节(比如主站的 IP 地址为 192.168.0.100。那么此字节就表示 192)。

第 3 字节：ModbusTCP 主站的 IP 地址第 2 字节(比如主站的 IP 地址为 192.168.0.100。

那么此字节就表示 168)。

第 4 字节：ModbusTCP 主站的 IP 地址第 3 字节(比如主站的 IP 地址为 192.168.0.100。那么此字节就表示 0)。

第 5 字节：ModbusTCP 主站的 IP 地址第 4 字节(比如主站的 IP 地址为 192.168.0.100。那么此字节就表示 100)。

其他字节保留。

Modbus 的控制字：

第一字节 QB128：

Bit 0：ModbusTCP 主站 1 和 ModbusTCP 从站使能位，1 = 启用，0 = 不启用。

Bit 1：ModbusTCP 主站 2 使能位，1 = 启用，0 = 不启用。

Bit 2：ModbusTCP 主站 3 使能位，1 = 启用，0 = 不启用。

Bit 3：ModbusTCP 主站 4 使能位，1 = 启用，0 = 不启用。

Bit 4：ModbusTCP 主站 5 使能位，1 = 启用，0 = 不启用。

Bit 5：ModbusTCP 主站 6 使能位，1 = 启用，0 = 不启用。

Bit 6：ModbusTCP 主站 7 使能位，1 = 启用，0 = 不启用。

Bit 7：ModbusRTU 主站和 ModbusRTU 从站使能位，1 = 启用，0 = 不启用。

正常使用时直接往第 1 字节中写入 255，即 8 个 1。

第 2 字节到第 9 字节：

每一个槽的报文对应一位。对应形式如下表。

当报文配置为上升沿触发时（见 4.6 章节 报文设置），将该位由 0->1 时，报文启用一次发送。

当报文配置为电平触发模式（见 4.6 章节 报文设置）。将该位置 1 时，对于写类型的功能码仅当数据发生变化时才发送，对于读类型的功能码会直接发送；置 0 时，报文停止发送。

PS:因硬件的原因，在使用的 Modbus TCP 的网口时，请勿用网线直接接入其它的 Modbus 的主站或者从站，需要中间接入一个交换机。

六、关于 PN2-MB-RT 网关设备的报警信息

当 PN2-MB-RT 网关出现错误时会通过 Profinet 的报警机制，将具体出错的信息发送给 PLC，同时网关的 ERR 灯会持续的三闪，PLC 的上的指示灯也会闪烁，当错误消失时,对应的报警信息就会被移除。可以通过 PLC 对应的上位机来查看具体的错误信息。

下面将具体的错误信息解释如下：

Illegal Fun Code [Slave] 表示 Modbus 主站发送的功能码不受支持或无效。

Illegal Data Address [Slave] 表示 Modbus 主站请求的数据地址超出了 Modbus 从站设备支持的范围，比如从站仅支持读取地址 0 和地址 1 两个字节的数据，但此时主站发送的设备数据起始地址为 2，那么就会报错。

Illegal Data Value [Slave] 表示 Modbus 主站请求的数据值无效或不符合设备的要求。

Slave Or Master Failure [Slave] 从设备故障，表示从设备无法执行请求的操作。

Acknowledge [Slave] 确认，表示设备接收到请求并正在处理。

Slave Or Master Busy [Slave] 从设备忙，表示从设备正在执行其他操作，无法立即处理请求。

Memory Parity Check Error [Slave] 内存奇偶校验错误，表示通信过程中发生了内存校验错误。

Gateway Path Error [Slave] 表示网关路径错误。

Target Gateway Error [Slave] 表示目标网关错误。

CRC Check Error [Slave] 表示 ModbusRTU 主站发送过来的数据 CRC 校验错误。

Protocol ID Error [Slave] 表示 ModbusTCP 主站发送过来的协议 ID 错误。

Frame Length Error [Slave] 表示 Modbus 主站发送过来的数据帧长度错误。

Unit Identifier Error [Slave] 表示 ModbusTCP 主站发送过来的单元标识符错误。

Coil Or Reg Num Error [Slave] 表示 Modbus 主站发送过来的线圈或寄存器个数超过了最大值。

Function Code Not Support [Slave] 表示 Modbus 从站暂时不支持主站发过来的功能码，比如从站中只有功能码 1,2 而主站发送了功能码 3，那么就会报这个错误。

Unknown Error [Slave] 表示 Modbus 从站发生了未知错误。

Unit Identifier Error [Master] 表示 ModbusTCP 从站发送过来的单元标识符错误。

Frame Length Error [Master] 表示 Modbus 从站发送过来的数据帧长度错误。

Protocol ID Error [Master] 表示 ModbusTCP 从站发送过来的协议 ID 错误。

Transfer ID Error [Master] 表示 ModbusTCP 从站发送过来的事务 ID 错误。

CRC Check Error [Master] 表示 ModbusRTU 从站发送过来的数据 CRC 校验错误。

SlReceive Timeout [Master] 表示 Modbus 主站接收数据超时。

Socket Connect Error [Master] 表示 ModbusTCP 主站连接目标从站失败，可能原因是网线断了或从站不在线或相关 IP 地址填写错误。

Socket Send Error [Master] 表示 ModbusTCP 主站向从站发送数据失败，可能原因是网线断了或从站

不在线或相关 IP 地址填写错误。

Socket Read Error [Master] 表示 ModbusTCP 主站接收从站数据失败，可能原因是网线断了或从站掉线了。

DHCP Service Error 表示 ModbusTCP 主站或者从站从路由器动态获取 IP 地址失败。

[Slave] 表示这个错误是 Modbus 从站报告给 Modbus 主站的

[Master] 表示这个错误是 Modbus 主站本身发出的

部分错误信息对应的错误码(就是 Modbus 从站返回过来的错误码)

错误信息	错误码
Illegal Fun Code [Slave]	0x01
Illegal Data Address [Slave]	0x02
Illegal Data Value [Slave]	0x03
Slave Or Master Failure [Slave]	0x04
Acknowledge [Slave]	0x05
Slave Or Master Busy [Slave]	0x06
Memory Parity Check Error [Slave]	0x08
Gateway Path Error [Slave]	0x0A
Target Gateway Error [Slave]	0x0B
上面是 Modbus 标准错误,下面是自定义的错误	
CRC Check Error [Slave]	0x80
Protocol ID Error [Slave]	0x81
Frame Length Error [Slave]	0x82
Unit Identifier Error [Slave]	0x83
Coil Or Reg Num Error [Slave]	0x84
Function Code Not Support [Slave]	0x85

修订历史

版本	修订日期	修订说明	维护人
V1.0	2024.5.21	初始版本	WH

关于我们

企业名称：东莞市艾莫迅自动化科技有限公司

官方网站：www.amsamotion.com

技术服务：4001-522-518 拨 1

企业邮箱：sale@amsamotion.com

公司地址：广东省东莞市南城区袁屋边艺展路 9 号兆炫智造园 B 栋 1 楼

官方公众号

官 方 抖 音